

## IPv6

FortiGate devices provide UTM and next generation firewall protection for IPv6 and extended IPv6 networking features such as, NAT64, DNS64, NAT66 and policy routing

FortiOS has been successfully evaluated as compliant with core protocol and interoperability tests defined by IPv6 Ready Logo Phase 2 (<http://www.ipv6ready.org>). Conformance to the latest test specifications and underlying RFCs provides the confidence needed to deploy FortiGate solutions in existing IPv6 networks, or IPv4 networks being prepared for transition.



### Why use IPv6?

IPv6 handles issues that weren't around decades ago when IPv4 was created—running out of IP addresses, fair distribution of IP addresses, built-in quality of service features (QoS), better multimedia support, and improved handling of fragmentation. The bigger address space, bigger default packet size, and more optional header extensions of IPv6 provide these features with flexibility to customize them to any needs.

IPv6 has 128-bit addresses compared to the 32-bit addresses of IPv4, effectively eliminating address exhaustion. This new very large address space will likely reduce the need for network address translation (NAT), since IPv6 provides more than a billion IP addresses for each person on Earth.

### Mixed IPv4 and IPv6 networks

For a lengthy period networks will have to support both IPv4 and IPv6. The transition will not happen over night simply because of the time required to convert equipment and applications to IPv6. In addition, some legacy equipment and applications may never support IPv6, and will have to either be replaced or will require ongoing support as IT budgets permit.

During this transition period, most networks will need to support both IPv6 and IPv4. Most networks will become mixed networks that have to understand and route both IPv6 and IPv4 addresses.

To be able to support both IPv6 and IPv4, FortiOS implements a dual stack architecture that recognizes and separately routes both address types. In addition to routing, most vital FortiOS network and content protection security features now fully support for IPv6.

### UTM and next generation firewall protection for IPv6 networks

Maintaining security for both types of traffic will be crucial to the success of IPv6 and mixed networks. Malware and network threats are independent of IPv4 or IPv6. FortiOS uses IPv6 security policies to provide UTM protection for IPv6 traffic. Antivirus, web filtering, FortiGuard Web Filtering, application control, IPS, email filtering, FortiGuard Email Filtering, data leak prevention (DLP), and VoIP protection can be enabled in IPv6 security policies using normal FortiOS UTM profiles for each UTM feature. This protection is transparent to IPv6 Users.

UTM support for IPv6 makes the transitional mixed network phase easier, because the level of security of transitional networks is extended to both IP protocols. Future releases of FortiOS will continue to extend IPv6 UTM protection.

## Supported IPv6 features

FortiOS 5.0 supports the following FortiOS IPv6 features:

- Static routing
- RIPv6, BGP4+, and OSPFv3
- Policy routing
- DNS
- Network interface addressing manually or using DHCPv6
- DHCPv6 relay
- Routing access lists and prefix lists
- IPv6 tunnel over IPv4, IPv4 tunnel over IPv6
- IPv6 NAT including NAT64, DNS64, and NAT66
- IPv6 Security policies
- Authentication
- IPv6 hardware acceleration with XG2 or XHO processors
- IPv6 over SCTP
- Packet and network sniffing
- IPsec VPN
- SSL VPN
- Proxy and flow-based UTM protection
- NAT/Route and Transparent mode
- Logging and reporting
- SNMP
- Virtual IPs and groups
- IPv6 specific troubleshooting such as ping6
- Explicit web proxying
- IPv6 MIB fields
- Per-IP traffic shaping
- HA session failover

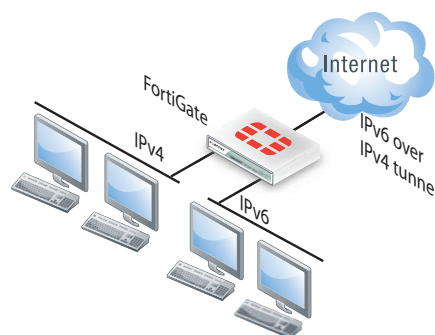
## FortiOS enables IPv6 solutions

### Solution 1 - Mixed internal network with both IPv4 and IPv6 traffic

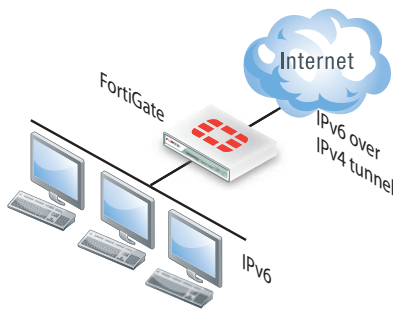
During the transition to IPv6, many organizations will continue to operate mixed internal networks that include both IPv4 and IPv6 devices. The FortiOS dual stack architecture supports both IPv4 and IPv6 traffic and routes the appropriate traffic as required to any device on the network. Administrators can update network components and applications to IPv6 on their own schedule, even maintaining some IPv4 support indefinitely if necessary.

Devices on a mixed network that connect to the Internet can query Internet DNS servers for IPv4 and IPv6 addresses. If the Internet site supports IPv6, the device can connect using the IPv6 address. If the Internet site does not support IPv6, then the device can connect using the IPv4 address. The dual stack architecture of FortiOS provides routing, security policies, and UTM security for all traffic on mixed networks.

If an organization with a mixed network uses an Internet service provider that does not support IPv6, they can use an IPv6 tunnel broker to connect to IPv6 addresses on the Internet. FortiOS supports IPv6 tunnelling over IPv4 networks to tunnel brokers. The tunnel broker extracts the IPv6 packets from the tunnel and routes them to their destinations.



## Solution 2 - IPv6 internal network connecting to the Internet



In this scenario, a company has completed the transition to IPv6 on their internal networks. All devices on the organization's networks support IPv6 and traffic among devices on the network uses IPv6 for all communications. FortiGate units can be assigned IPv6 addresses, deployed on IPv6 networks, include IPv6 static and dynamic routing, authentication, and IPv6 security policies with UTM functionality.

However, since many Internet services do not support IPv6, even internal networks that completely support IPv6 require the dual stack architecture of FortiOS to connect to IPv4 addresses on the Internet. Networks that have completed the transition to IPv6 may still require tunneling IPv6 over IPv4 to

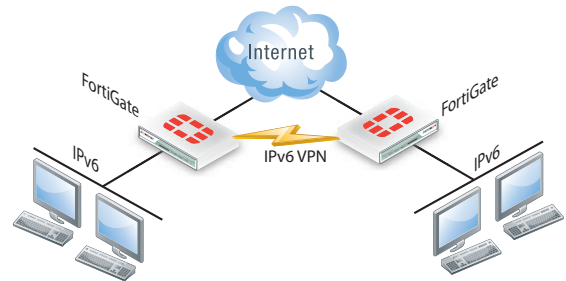
reach IPv6 addresses on the Internet.

FortiOS 5.0 now also supports NAT64 and DNS64 allowing users on a IPv6 internal network to transparently connect to IPv4 addresses on the Internet. NAT64 and DNS64 transparently translates addresses from IPv6 to IPv4 before sending packets across the internet and re-translates addresses from IPv4 to IPv6 before the packets return to the internal network.

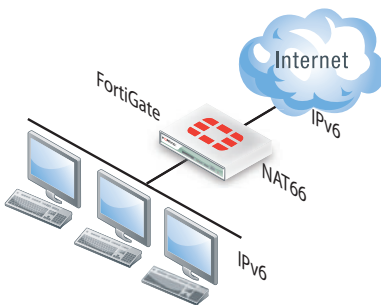
## Solution 3 - IPv6 network connecting to a remote IPv6 network over the internet

Similar to the IPv6 over IPv4 tunnelling, FortiOS supports IPv6 tunnelling over IPv4 across the Internet between two IPv6 networks protected by FortiGate units. All traffic between the IPv6 networks can be tunnelled over IPv4. Each FortiGate unit extracts the IPv6 traffic from the IPv4 tunnel and Traffic on the internal networks uses IPv6.

FortiOS also supports tunnelling IPv6 traffic over an IPsec VPN between two IPv6 networks protected by FortiGate units. The VPN provides higher security for the data transmitted between the networks. Configuration of this topology involves configuring an interface-based IPsec VPN between IPv6 interfaces on each FortiGate unit.



## Solution 4 - IPv6 NAT (NAT66)



In this scenario, a company wants to hide the IPv6 addresses on its internal network from the Internet or from another network. To do this, the company configures the FortiGate unit to use NAT66 in the same way as many IPv4 networks hide their private network addresses by using IPv4 NAT.

For communication from the internal network to IPv6 addresses on the Internet, the FortiGate unit translates source addresses to the FortiGate external interface address before forwarding packets across the Internet. The destination address of return packets is translated from the FortiGate external interface address back to the address of the originator of the communication session.

NAT66 allows organizations to hide the IPv6 addresses of their internal networks and to also use their own internal IPv6 addressing independently of their public IPv6 addresses.

## Conclusion

All hardware and software network components must support the IPv6 address size—an upgrade that will take time to complete and will force IPv6 and IPv4 to work side-by-side during the transition period. FortiOS support of IPv4 and IPv6, including full UTM protection for both, will ensure a smooth transition for networks with minimal or no impact to your users.